2008年7月2日

情報セキュリティ大学院大学
情報セキュリティ研究科（博士前期課程）情報セキュリティ専攻
2009年度特待生選抜試験問題

1次選考（筆記試験）

10:00～11:30

Ⅰ数学A
Ⅱ数学B
Ⅲ通信ネットワーク
Ⅳ情報システム
Ⅴソフトウェア
Ⅵ暗号技術
Ⅶ経済
Ⅷ経営
Ⅸ法律

【注意事項】

1. 指示があるまで、この問題冊子を開いてはならない。
2. この問題冊子の本文は全部で20ページある。落丁、乱丁があれば申し出ること。
3. 上記Ⅰ～Ⅸの9項目から2項目を選択し、解答すること。9項目中どの2項目を選択してもよい。
4. 解答用紙は2枚配布される。選択した項目ごとに解答用紙を1枚使用すること。必要があれば裏面を使用してよい。
5. 解答用紙の指定欄に、選択した項目名、受験番号を必ず記入すること。解答用紙の回収前に、これらを記入したかを必ず確認すること。
6. 問題冊子、解答用紙、計算用紙は持ち帰ってはならない。

I 数学 A

素数 $p = 13$ に対し、$K = \mathbf{Z}/p\mathbf{Z}$ とし、$a = 2 \in K$ とする。多項式 $f(x) \in K[x]$ を

$$f(x) = 6x^4 + 9x^3 + x^2 + 10x + 5$$

と定める。また、$f(x)$ の k 次係数を f_k と表し、$n = \deg f(x) = 4$ とする。以下の問いに答えよ。

(1)

$$r_k \equiv k! \bmod p$$

かつ $0 \leq r_k \leq p-1$ を満足する整数 r_k を $1 \leq k \leq p-2$ に対して求めよ。次に、

$$r_k s_k \equiv 1 \bmod p$$

かつ $0 \leq s_k \leq p-1$ を満足する整数 s_k を $1 \leq k \leq p-2$ に対して求めよ。

(2) (1) で求めた r_k, s_k を K の元であると考える。また、$r_0 = s_0 = 1 \in K$ とする。$0 \leq k \leq n$ に対し、

$$u_k = r_{n-k} f_{n-k} \in K$$

と

$$v_k = a^k s_k \in K$$

を求めよ。

(3) (2) で求めた $u_k, v_k \in K$ $(0 \leq k \leq n)$ によって、多項式 $u(x), v(x) \in K[x]$ を、$u(x) = \sum_{k=0}^{n} u_k x^k$, $v(x) = \sum_{k=0}^{n} v_k x^k$ と定める。

$$w(x) \equiv u(x)v(x) \bmod x^{n+1}$$

かつ $\deg w(x) \leq n$ を満足する多項式 $w(x) \in K[x]$ を求めよ。

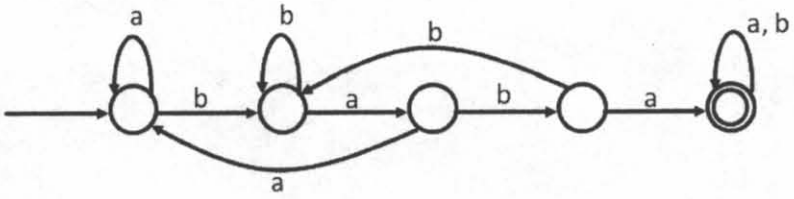
(4) $f(x)$ の j 階形式微分を $f^{(j)}(x)$ と表し、特に $f^{(0)}(x) = f(x)$ とする。$0 \leq j \leq n$ に対し、$f^{(j)}(a) \in K$ を求めよ。

(5) 多項式 $f(x+a) \in K[x]$ を求めよ。

II 数学 B

決定性有限オートマトン (DFA) について、以下の問いに答えよ。

(1) 以下の (状態数 5 の)DFA が受理する言語を求めよ。(ラベルのない矢印は開始状態を指し、2 重丸は終了状態を表す。)



(2) 状態数 7 のある DFA で受理され、状態数 6 以下のどのような DFA によっても受理されない言語の例を示せ。

(3) 言語 $L = \{ww \mid w \in \{a, b\}^*\}$ を受理する DFA は存在しないことを示せ。

III 通信ネットワーク

下記の文章を読んで（1）から（4）に答えよ。

「インターネットのようなパケット通信では、ウェブやメール等のアプリケーションデータ（データと呼ぶ）を送信側である長さに分割し、アドレスなどの制御情報を付加したパケットとして転送する。このように、(A) パケットはデータ部（ペイロードと呼ぶ）と制御情報部（ヘッダと呼ぶ）から成っている。 (B) 転送の信頼性を保つため、受信側では正しくパケットが転送されたか否かを検査し、(C) 受信確認情報をヘッダに挿入して（このパケットを Ack パケットと呼ぶ）を送信側に返す。しかし、このような (D) 受信確認を行わないアプリケーションも増えている。」

（1）下線部 (A) について、ヘッダ長が固定の場合、ペイロード長を小さくすると、パケットにおけるヘッダの占める割合が大きくなり、転送効率が劣化する。したがって、ペイロード長を大きく、すなわち、パケット長をできるだけ大きくする方が転送効率の点で望ましい。しかし、実際には、パケット長の最大値を定めている。この理由について説明せよ。

（2）下線部 (B) について、正しくパケットが転送されない原因としてどのようなものが考えられるか。二つ示せ。

（3）下線部 (C) について、送信側ではある時間以上たっても、受信側から Ack パケットが送られてこない場合、以前送信したパケットを再送する。これをタイムアウト再送と呼ぶ。タイムアウト再送を行う場合の時間のしきい値は通信経路毎に設定される。このしきい値はどのように設定されるか説明せよ。

（4）下線部 (D) について、受信確認を行わないアプリケーションの例を一つあげよ。また、その例において、受信確認を行わない理由を示せ。

Ⅳ情報システム

次の項目すべてについて、それぞれ６行程度で説明せよ。

（１）コンピュータ・プロセスとは何か
（２）仮想記憶の目的とそれを実現する仕組みの概要
（３）キャッシュを使うと処理が高速化されるメカニズム
（４）プロセス実行の相互排除（排他）とは何か、またそれが必要となる具体例
（５）コンピュータにおける内部割り込みと外部割込み、それぞれの目的

Vソフトウェア

[問題]
テキスト文字列の中から、特定の文字列（パターン）を探索する方法を考える。
テキスト文字列をテキスト配列 text[i] (i=0, 1, 2, …… , tl-1)、特定の文字列をパターン配列 pattern[j] (j = 0,1,2,…… ,pl-1)とする。文字列の探索とは、配列 text 内に配列 pattern と一致する部分文字列を見つけ、そのときの部分文字列の先頭の添字を求めることである。
テキストおよびパターンの文字数を　tl = 19, pl=3 とした場合の例を図 1 に示す。

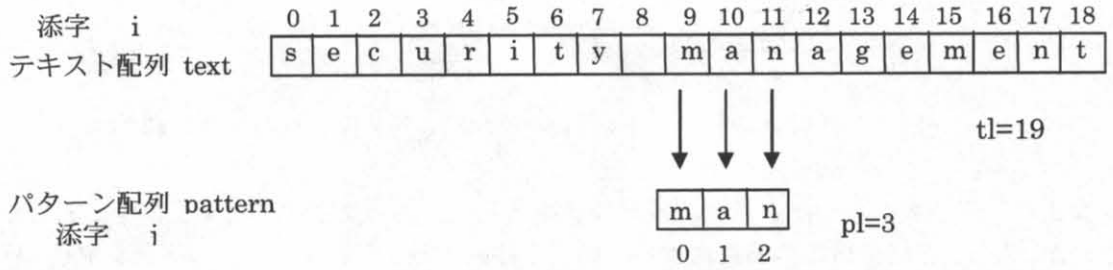


図 1　文字列検索の例

パターンと一致する文字列がない場合は match = 0 とし、文字列がある場合は match=1 とするとともに先頭の添字を求める。　テキスト内にパターンと一致する部分文字列が複数ある場合は、もっとも左側（添字の小さい方）のものを結果とする。

このような文字列検索の方法として、Boyer-Moore の文字列探索方法がある。この方法の考え方は、以下のとおりである。
ある箇所で一致する見込みがないとわかれば、大きく移動する方が効率が良い。まずテキストの先頭の pl 文字を比較対象テキストとする。比較対象テキストとパターンが図 2 のような場合を考える。最初に比較するのは、パターンの最後の文字 「n」と、比較対象テキストの最後の文字「c」である。この二つは一致しないので比較対象テキストを右に一つないしは二つ移動して再度比較する。しかし、「c」 は 「a」とも 「m」とも一致しない。つまり、1 文字移動しても、2 文字移動してもパターンとは一致しない。そのため比較対象テキストを一挙に 3 文字移動してよいことがわかる。

図 2　比較対象テキストにパターンの文字が含まれない場合の移動

次に比較対象テキストとパターンが図３のような場合を考える。この場合は比較対象テキストを２文字移動すれば、一致する可能性のあることがわかる。

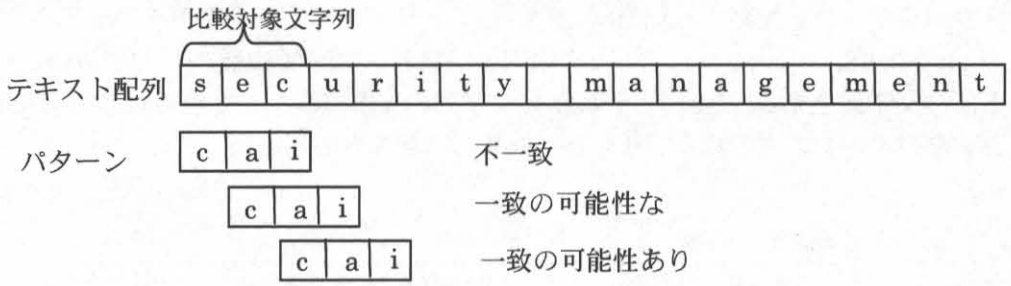


図３　比較対象テキストにパターンの文字が含まれる場合の移動

つまり、不一致となったときの比較対象テキストの最後の文字ｘがパターン中にあるかどうか、かつ、どの位置にあるかによって何文字移動するかが決まる。この移動文字数（移動距離　d[x]）をテキスト中のすべての文字についてあらかじめ計算をしておく。図２の場合の移動距離 d[x]は表１のとおりである。

比較対象テキストの最後の文字 x	パターン中に存在する文字			パターン中に存在しない文字
	m	a	n	
移動距離 d[x]	2	1	3	3

表１　　パターンが「man」のときの移動距離 d[x]

以上の方法でのアルゴリズムは次のとおりである。

① 比較対象テキストとパターンを後ろから前に向かって１文字ずつ照合する。
② 完全に一致した場合は、match= 0 とするとともに比較対象テキストの先頭の添字 i の値を返す。
③ 一致しない場合は、比較対象テキストの末尾の文字 x に対する移動距離 d[x]分だけ比較対象テキストを移動する。

問題

（１）　この方法の C++で作成したプログラムを図４に示す。（移動距離 d[x]の計算は、文字が１バイトコードの場合に限定している）
図中の（あ）（い）（う）（え）（お）に適切な字句を入れなさい。

（２）　このプログラムで一致しなかった場合、どのような値が返るか。

（３）　この探索で最も早く探索が終わるのは、テキストの先頭にパターンと一致する文字列があるときで、文字の比較回数は pl 回である。最悪の場合の比較回数は何回か？

（４）　どのようなテキスト配列とパターン配列が与えられたとき、上記(３)の回数の比較後失敗となるか。　tl=10, pl=3 のケースで　一例あげよ。

（５）　パターン中のどの文字もテキスト中に現れない場合、文字列の比較回数を求めよ。

```
void dist(int d[], int pattern[], int pl);

int textsearch(int text[], int pattern[], int tl, int pl){
    int i, j, match;
    int d[256];
// 移動距離の計算
    dist(d, pattern, pl);
//  テキストサーチ
    match = 0;
    i = [      (あ)      ]
    while (match == 0 && i < tl) {                    //開始点移動ループ
        j = pl - 1;
        while (  [      (い)      ]  ) {              // 照合開始ループ
            j--;
            i--;
        }
        if( j>= 0) {                                  //照合失敗
            i = i + [      (う)      ]
            i = i + d[text[i]];
        }else {                                       //照合成功
            match = 1;
            [      (え)      ]
        }
    }
    return i;
}

void dist(int d[], int pattern[], int pl){
    int i;
    int dmax= 256;          // 1バイトコード

    for(i=0;i < dmax; i++){   d[i] = pl; }
    for (i= 0;i < pl - 1; i++) { [      (お)      ]    }
}
```

図4　　Boyer-Moore の文字列探索プログラム

VI 暗号技術

p, q を奇素数，$n = pq$，$\phi(n) = (p-1)(q-1)$ とする．$\gcd(\phi(n), e) = 1$ となる整数 e をランダムに選び，d を $ed \equiv 1 (\mathrm{mod} \phi(n))$ となる整数とする．また，関数 E, D を

$$E(m, e, n) = m^e \bmod n \tag{1}$$

$$D(c, d, n) = c^d \bmod n \tag{2}$$

とする．すると，(n, e) を公開鍵，d を秘密鍵とし，暗号化関数を E，復号関数を D とすることにより，公開鍵暗号方式 (以下，方式 1) を構成できる．各設問に答えよ．

問 1 任意の $m \in (\mathbf{Z}/n\mathbf{Z})^*$ について，$D(E(m, e, n), d, n) = m$ となることを示せ．

問 2 方式 1 は選択平文攻撃のもとで識別不可能性を有しないことが知られている．識別不可能性の定義を与えるとともに，このことを示せ．

問 3 公開鍵 (n, e) 及び $\phi(n)$ が与えられたとき，p, q を計算する方法を示せ．

問 4 $p = 7, q = 13, e = 5$ とする．

(a) $ed \equiv 1 (\mathrm{mod} \phi(n))$ となる d を求めよ．

(b) $c = 19$ に対して，$D(c)$ を求めよ．

Ⅶ経済

次の各語の意味するところについて、具体例を用いて、それぞれ15行程度で説明せよ。

(1) 情報の非対称性

(2) プリンシパル・エージェント・モデル

Ⅷ経営

次の項目すべてについて、企業経営の観点で、各々10行程度で説明せよ。

(1) 顧客満足度

(2) M&A

(3) 管理会計と財務会計

IX法律

情報に関連する法律を１つ選択し、その概要を説明せよ。解答にあたっては、当該法律の目的、適用対象、権利・義務、違反行為に対する制裁に分け、該当条文を取り上げること。　*六法使用可